**Amendments to the Specification**

Please replace paragraph [0003] with the following amended paragraph:

[0003] Certain efficiencies may be realized in cryptographic operations by choosing a particular set of bases for that finite field. For example, in the finite field $F(2^n)$, two common choices of bases [[of]] are the polynomial basis and a normal basis. A problem arises though in the choice of basis since communication between the two parties, although using the same cryptographic scheme but having different bases elements, requires the parties to perform a basis conversion operation on the field elements in order to obtain the same cryptographic result.

Please replace paragraph [0007] with the following amended paragraph:

[0007] Various techniques have been implemented to convert between two choices of [[basis]] bases for a finite field. A conventional approach involves using a matrix multiplication, wherein basis conversion is performed using a change of basis matrix m, resulting in a matrix of size $m^2$. If m is typically 160 bits, then this occupies significant storage in devices such as a smart card. General finite field techniques are described in the "Handbook of Applied Cryptography", CRC Press, 1996 by S. A. Vanstone et al and incorporated herein by reference. Other techniques for basis conversion are described in U.S. Pat. No. 5,854,759 to Kaliski et al, also incorporated herein by reference.

Please replace paragraph [0014] with the following amended paragraph:

[0014] In a first embodiment, shown in FIG. 1 a pair of correspondents are represented by A and B and an intermediate processor, such as a server, certifying authority or other helper processor, [[is]] represented by H. It is assumed the correspondents A and B include processors for performing cryptographic operations and the like that may be implemented in hardware or in software operated on a general purpose computer. In this case the software may be encoded as a data carrier such as a CD ROM or computer disk for loading on to the computer. Specifically, A and B perform cryptographic operations [[n]] in a basis $\beta_1$ and $\beta_2$, respectively. It is further

Best Available Copy

assumed that the respective cryptographic parameters are contained within the entities A and B. For example in an elliptic curve scheme the system parameters include at least a point P on the elliptic curve, the order of the curve and the parameters of the elliptic curve equation E.

Please replace paragraph [0015] with the following amended paragraph:

[0015] In this embodiment, each of the entities A and B generates a respective random value $k_i$, generally the private session key and each computes a public value $[[k_iP]]$ $k_iP$, represented in terms of their respective bases $\beta_1$ and $\beta_2$. One of the entities, A for example, transmits its public key $kP_{\beta 1}$ to the server H. The server H performs a basis conversion utilizing one of many basis conversion algorithms to convert the public key $kP_{\beta 1}$ represented in basis $\beta_1$ to a public key $kP_{\beta 2}$ represented in terms of the basis $\beta_2$. The converted key is transmitted back to the correspondent A. The correspondent A then computes signature $s=k^{-1}(h(m)+dr)$, where $r=kP_{\beta 2}$. The signature s and r are then transmitted to the other correspondent B, which is then processed by B in the basis $\beta_2$. Similarly if correspondent B wishes to communicate with A it also transmits its public key $kP_{\beta 2}$ to the server, which performs the conversion on the key and sends it back to the correspondent B. The correspondent B also computes a signature using $r=kP_{\beta 1}$.

Best Available Copy